PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PU 030082	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. PCT/US04/07411	International filing date *(day/month/year)* 11 March 2004 (11.03.2004)	Priority date *(day/month/year)* 14 March 2003 (14.03.2003)
International Patent Classification (IPC) or national classification and IPC IPC(7): G06F 15/16 and US Cl.: 709/228		
Applicant THOMSON LICENSING S.A.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 2 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☒ *(sent to the applicant and to the International Bureau)* a total of 14 sheets, as follows:
      ☐ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s))
      ____ , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).
4. This report contains indications relating to the following items:
   - ☒ Box No. I Basis of the report
   - ☐ Box No. II Priority
   - ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - ☐ Box No. IV Lack of unity of invention
   - ☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - ☐ Box No. VI Certain documents cited
   - ☐ Box No. VII Certain defects in the international application
   - ☐ Box No. VIII Certain observations on the international application

Date of submission of the demand 11 January 2005 (11.01.2005)	Date of completion of this report 07 February 2005 (07.02.2005)
Name and mailing address of the IPEA/ US Mail Stop PCT, Attn: IPEA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer John A Follansbee Telephone No. (703)305-3900

Form PCT/IPEA/409 (cover sheet)(January 2004)

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US04/07411

Box No. I Basis of the report

1. With regard to the language, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ This report is based on translations from the original language into the following language _____, which is the language of a translation furnished for the purposes of:

☐ international search (under Rules 12.3 and 23.1(b))

☐ publication of the international application (under Rule 12.4)

☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the elements of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

☐ the international application as originally filed/furnished

☒ the description:
pages NONE as originally filed/furnished
pages* 1-7 received by this Authority on 11 January 2005 (11.01.2005)
pages* NONE received by this Authority on _____

☒ the claims:
pages NONE as originally filed/furnished
pages* NONE as amended (together with any statement) under Article 19
pages* 8-11 received by this Authority on 11 January 2005 (11.01.2005)
pages* NONE received by this Authority on _____

☒ the drawings:
pages NONE as originally filed/furnished
pages* 1-3 received by this Authority on 11 January 2005 (11.01.2005)
pages* NONE received by this Authority on _____

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages_____
☐ the claims, Nos._____
☐ the drawings, sheets/figs_____
☐ the sequence listing (*specify*): _____
☐ any table(s) related to the sequence listing (*specify*):_____

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

☐ the description, pages_____
☐ the claims, Nos._____
☐ the drawings, sheets/figs_____
☐ the sequence listing (*specify*): _____
☐ any table(s) related to the sequence listing (*specify*):_____

** If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US04/07411

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1-22	YES
	Claims NONE	NO
Inventive Step (IS)	Claims 1-22	YES
	Claims NONE	NO
Industrial Applicability (IA)	Claims 1-22	YES
	Claims NONE	NO

2. Citations and Explanations (Rule 70.7)

Claims 1-22 the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest that the claimed dialogue runs between the user/mobile client terminal and an access point. The Hsu reference teaches the challenge and response dialog running between the MSC and the mobile device.

Claims 1-22 meet the criteria set out in PCT Article 33(4), and thus a method that is useful for exchanging administration management information between access point and client terminal in an industrial applicability because the subject matter claimed can be made or used in industry.

---------- NEW CITATIONS ----------

SECURE WEB BROWSER BASED SYSTEM ADMINISTRATION FOR EMBEDDED PLATFORMS

RELATED APPLICATION

This application claims the benefit of U.S. Provisional Application No. 60/454,582, filed March 14, 2003, and incorporated herein by reference.

1. Field of the invention

The invention relates to a method for providing configuration changes in a network access point, and in particular, provides a method in a WLAN environment where an access point and a stationary computer or a mobile terminal maintaining a web browser utilizes an ActiveX control or a plug-in to enhance a security mechanism without relying on HTTPS protection during remote management and administration processing.

2. Description of Related Art

The context of the present invention is to securely access networks, such as the World Wide Web, through another network, including wireless local area networks or (WLAN), having an access point that provides access for a stationary computer or a mobile terminal devices and to other networks, such as hard wired local area and global networks, such as the Internet. Advancements in WLAN technology have resulted in the publicly accessible wireless communication at rest stops, cafes, libraries and similar public facilities ("hot spots"). Presently, public WLANs offer mobile communication device users access to a private data network, such as a corporate intranet, or a public data network such as the Internet, peer-to-peer communication and live wireless TV broadcasting. The relatively low cost to implement and operate a public WLAN, as well as the available high bandwidth (usually in excess of 10 Megabits/second) makes the public WLAN an ideal access mechanism, through which, mobile wireless communications device users can exchange packets with an external entity. However as will be discussed below, such open deployment may compromise security unless adequate means for identification and authentication exists during regular communications and in processing remote management and administrative functions.

In a web browser based authentication method, a stationery computer or a mobile terminal communicates with an access point (AP), using a web browser operating with the Hyper Text Transfer Protocol Secured Sockets (HTTPS) protocol insures that anyone on the

path between the mobile terminal and the AP cannot trespass upon or steal confidential user information.

Remote system management/administration is a key requirement on any type of computer systems. Using web browsers (HTTP protocol) as the interface for remote management is becoming an essential management feature. In order to provide secure browser based remote management, HTTPS is the natural choice. However, for embedded systems, such as WLAN access points, the resource requirement on HTTPS may be too great consuming large amounts of storage space and requires corresponding overhead support and CPU power. In fact these limitations have historically prevented the development of a practical solution to a secure browser based administration mechanism. For example, most of today's commercially available wireless access points do not protect the remote administration exchanges between the browsers and the access points. A would be hacker might easily obtain administrator passwords and damage the access points.

HTTPS is designed for communication protocols where neither a browser nor a web server have pre-established authentication codes such as confidential passwords known only by the client terminal and the authentication server. This assumption of confidentiality is absolutely necessary in the web applications in which tens of millions of browsers may access millions of servers, but do not have a prior trust relationship. Thus a large use HTTPS requires a certificate on the server to provide a secure negotiation between the browser and the server, and the establishment of a shared secret code for subsequent HTTP communication. In the remote system administration case, the administrator and the remote device can pre-share a secret, thus removing one source of overhead associated with HTTPS communication. However, since the web browser does not offer the necessary secure communication mechanism based on such a shared secret, it would be a desirable feature for a processor to provide the security through the use of an ActiveX control or functionally equivalent plug-in.

SUMMARY OF THE INVENTION

The invention herein provides a method for improving security during a remote administration exchange between a client device using a browser and an access point of a network. In particular, the invention provides a method for securely exchanging administration change requests between a client device and an access point of a wireless network (WLAN). The WLAN may comprise a network that complies with IEEE 802.11 standards. The administration change involves the use of parameters for ensuring that received administration information is received from an appropriate client terminal. Generally, when a request for administration management file, such as a web page, is received, the access point of the network also generates and transmits to the client terminal a first parameter, for example, a random number. The first parameter may be generated in response to a challenge following the request for the administration management file.

Using a predetermined algorithm, such as the MD5 hash function, a new parameter is generated from certain parameters. The parameters may include the first parameter, which may be a random number generated by the access point. For greater security, the new parameter may be generated from several parameters, including a password associated with the client terminal, the first parameter, and a string parameter, which may, for example, be generated from the new administration information. The new parameter is transmitted from the client terminal to the access point, which then generates a corresponding new parameter using the parameters used by the client terminal. If the parameters match, the access point accepts the new administration information and implements them. In this manner, greater security is provided by using a verification parameter with the new administration information, which verification parameter is generated using parameters that are known to the client terminal and the access point.

In an embodiment of the present invention an administrator utilizes a browser to request an administrative web page form, typically designed as a Hyper Text Markup Language (HTML) form, from a remote embedded platform, such as an AP, which contains fields where the administrator can provide information relevant to obtaining a secure communication with the network. The web page form includes fill-in management information, which when complete is submitted to the remote embedded platform by invoking a real time operator, such as may be provided by a Javascript code, to package the information

into a string. The real time operator invokes a plug-in security function having a predetermined character string as one parameter; prompting the security function to communicate with a remote system.

Upon receiving a request from the plug-in on the user/mobile terminal, the remote system generates a random number and stores the number for future reference. It also communicates the number to the administrator. The administrator security function concatenates the random number, an administrator password (previously stored in the plug-in) and the string parameter. Thereafter, a digest, such as a Message 5 digest (MD5), is generated for the concatenated result and is returned to the security function. The process includes utilizing the real time operator such as Javascript to then embed the result from the security function into the form containing the management information and sends the form to the remote computer, thereby completing the submission. The remote computer utilizes the stored random number, the password and the received data to generate an MD5 digest. If the digest matches the received digest then the requested administration is granted and the system is appropriately updated. In subsequent communication where management information is to be communicated from the administrator to the remote computer, the remote computer first generates a random number to be thereafter utilized by the administrator in a Message 5 digest (MD5). In each case, the remote system digest is then compared to the received digest and if the digest matches the received digest, then the requested administration request is granted and the system is updated accordingly.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is best understood from the following detailed description when read in connection with the accompanying drawing. The various features of the drawings are not specified exhaustively. On the contrary, the various features may be arbitrarily expanded or reduced for clarity. Included in the drawing are the following figures:

FIG. 1 is a block diagram of a communications system for practicing the method of the present invention.

FIG. 2 is a flow diagram of an embodiment of the present invention for securing a communication access.

FIG. 3a is a flow diagram of an embodiment of the present invention for securing a communication access.

FIG. 3b is a flow diagram of an embodiment of the present invention for securing a communication access.

DETAILED DESCRIPTION OF THE INVENTION

In the figures to be discussed the circuits and associated blocks and arrows represent functions of the process according to the present invention which may be implemented as electrical circuits and associated wires or data busses, which transport electrical signals. Alternatively, one or more associated arrows may represent communication (e.g., data flow) between software routines, particularly when the present method or apparatus of the present invention is implemented as a digital process.

The invention provides a method for a web browser based remote administration system to maintain its security by utilizing an ActiveX control or a plug-in, without relying on HTTPS protection to transact management information. The invention does not burden the embedded system and thus is ideally suited for the remote administration of embedded systems. The invention provides a method to calculate a security code base upon identical algorithms in the administrative system having the browser and the embedded system. When the browser-based administrator submits the management information, an operator packages the control information as a string and invokes the security function in the plug-in with the string as a parameter. After the security function returns the result, the operator sends the form data together with a coded digest to the remote system. The digest may be embedded in the form data, for example, as a hidden field.

In accordance with FIG. 1, one or more mobile terminals represented by 140_1 through 140_n communicate via wireless medium 124 to an access point 130_n, local computer 120, in association with firewalls 122 and one or more virtual operators 150_{1-n}, such as authentication server 150_n. Communication from terminals 140_{1-n} typically require accessing a secured data base or other resources, utilizing the Internet 110 and associated communication paths 154

and 152 that require a high degree of security from unauthorized entities, such as would be hackers.

In accordance with the present principles, the an access 160 enables each stationary or mobile terminals 140_{1-n}, to securely access the WLAN 115 by authenticating and thereafter providing a means to create the administrative forms that ensure a secure traffic flow between both the terminal as well as its communication system components, through such gateways 121, firewalls 122 that may exist as part of the larger network and communication paths 152 and 154 which denote HTTP and non-HTTP communication routing. The manner in which the access 160 enables such secure access can best be understood by reference to FIG. 1.

More specifically, with reference to FIG. 2 and FIG. 3a, a method in accordance with the present invention an administrator utilizes terminals 140_{1-n} and a browser to request 210 an administrative web page form, typically designed as an Hyper Text Markup Language (HTML) form, from a remote 150 embedded platform (e.g., AP 130), which contains fields where the administrator can provide information relevant to change configuration settings with the network. Upon receiving the form 215, the web page form filled-in with requested management information, which when complete 220 is submitted 225 to the remote embedded platform (e.g., AP 130) by invoking a real time operator, such as may be provided by a JavaScript code, to package 230 the information into a string. The real time operator invokes a plug-in security function 235 having a predetermined character string as one parameter; prompting 240 the security function to communicate 250 with a remote embedded platform (e.g., AP 130).

After making the necessary configuration change(s), the user/mobile terminal requests a random number (RN). Upon receiving the random number request 320, the remote embedded platform (e.g., AP 130) generates a random number 330, forwards the RN to the user/mobile terminal and stores the number 335 for future reference. It also communicates 340 the number to the administrator 140_{1-n}. The administrator 140_{1-n} security function concatenates 260 the random number, an administrator password (previously stored in the in the plug-in) and the string parameter. Thereafter, a digest, such as a Message 5 digest (MD5), is generated 270 for the concatenated result and is returned to the security function. The process includes utilizing the real time operator such as JavaScript to then embed the result from the security function into the form containing the management information and sends 275 the form to remote embedded platform (e.g., AP 130), thereby completing the

submission. The remote computer utilizes the stored random number, the password and the received data to generate 350 a MD5 digest. If the digest matches 355 the received digest then the requested administration is granted 360 and the system is appropriately updated. If there is no match access is denied 356. In subsequent communication where management information is to be communicated from the administrator to the remote embedded platform (e.g., AP 130), the remote embedded platform (e.g., AP 130) first generates a random number to be thereafter utilized by the administrator in a Message 5 digest (MD5). In each case, the remote system digest is then compared to the received digest and if the digest matches the received digest, then the requested administration request is granted and the system is updated accordingly.

It is to be understood that the form of this invention as shown is merely a preferred embodiment. Various changes may be made in the function and arrangement of parts; equivalent means may be substituted for those illustrated and described; and certain features may be used independently from others without departing from the spirit and scope of the invention as defined in the following claims.

We claim:

1. A method for exchanging administration management information with a client terminal in a wireless network, comprising the steps of:

receiving by an access point (AP) a request for an administration management file from the client terminal;

transmitting by the AP the administration management file to the client terminal;

generating by the AP and transmitting by the AP to the client terminal a first parameter;

receiving by the AP new administration information and a second parameter from the client terminal;

generating by the AP a third parameter using a predetermined algorithm and the first parameter;

comparing by the AP the third parameter to the second parameter; and

implementing the new administration information in response to the comparing step.

2. The method according to claim 1, wherein the wireless network is a wireless local area network (WLAN) in accordance with IEEE 802.11 standards, the client terminal is a mobile terminal within a coverage area of the WLAN, and the administration management file comprises an administration web page.

3. The method according to claim 2, wherein the first parameter is a random number.

4. The method according to claim 3, wherein the step of generating a third parameter comprises generating the third parameter using a hash function and the first parameter.

5. The method according to claim 3, wherein the step of generating a third parameter comprises generating a third parameter using a hash function, the first parameter, a password, and a string parameter.

6. The method according to claim 5, wherein the string parameter corresponds to the new administration information.

7. The method according to claim 2, wherein the transmitting step comprises transmitting the administration web page and Active X control to the client terminal.

8. An access point in a wireless network, comprising:

a transceiver for communicating with a client terminal;

means, coupled to the transceiver, for causing the transceiver to transmit an administration management file in response to a request from the client terminal,

means for generating a first parameter and causing the transceiver to transmit the first parameter to the client terminal, the transceiver receiving from the client terminal new administration information and a second parameter;

means for generating a third parameter in response to the first parameter, and comparing the third parameter to the second parameter; and

means for implementing the new administration information in response to the comparison.

9. The access point according to claim 8, wherein the wireless network is a wireless local area network (WLAN) in accordance with IEEE 802.11 standards, the client terminal is a mobile terminal within a coverage area of the WLAN, and the administration management file comprises an administration web page.

10. The access point according to claim 9, wherein the first parameter is a random number, and the means for generating a third parameter comprises means for generating the third parameter using a hash function, the random number, a password, and a string parameter.

11. The access point according to claim 10, wherein the string parameter corresponds to the new administration information.

12. A method for exchanging administration management information with an access point in a wireless network using a client terminal, comprising the steps of:

transmitting a request for an administration management file to the access point;

receiving the administration management file from the access point;

receiving a first parameter from the access point;

generating new administration information in response to user input;

generating a second parameter using a predetermined algorithm and the first parameter;

transmitting the second parameter and the new administration information to the access point.

13. The method according to claim 12, wherein the wireless network is a wireless local area network (WLAN) in accordance with IEEE 802.11 standards, the client terminal is a mobile terminal compliant with the IEEE 802.11 standards, and the administration management file is an administration web page.

14. The method according to claim 13, wherein the step of receiving the administration web page includes receiving the administration web page and an Active X control.

15. The method according to claim 13, wherein the step of generating a second parameter comprises generating the second parameter using a hash function and the first parameter.

16. The method according to claim 13, wherein the step of generating a second parameter comprises generating the second parameter using a hash function, the first parameter, a password and a string parameter.

17. The method according to claim 16, wherein the string parameter is generated from the new administration information.

18. A client terminal for communicating with an access point associated with a wireless network, comprising:

transceiver for communicating with the access point;

means coupled to the transceiver for causing the transceiver to transmit to the access point a request for an administration management file, and receiving the administration management file from the access point, and for receiving a first parameter from the access point;

means for generating new administration information in response to user input;

means for generating a second parameter using a predetermined algorithm and the first parameter;

means for causing the transceiver to transmit to the access point the second parameter and the new administration information.

19. The client terminal according to claim 18, wherein the wireless network is a wireless local area network (WLAN) in accordance with IEEE 802.11 standards, the client terminal is a mobile terminal compliant with the IEEE 802.11 standards, and the administration management file is an administration web page.

20. The client terminal according to claim 19, wherein the second parameter is generated using a hash function and the first parameter.

21. The client terminal according to claim 19, wherein the second parameter is generated using a hash function, the first parameter, a password and a string parameter.

22. The client terminal according to claim 22, wherein the string parameter is generated from the new administration information.

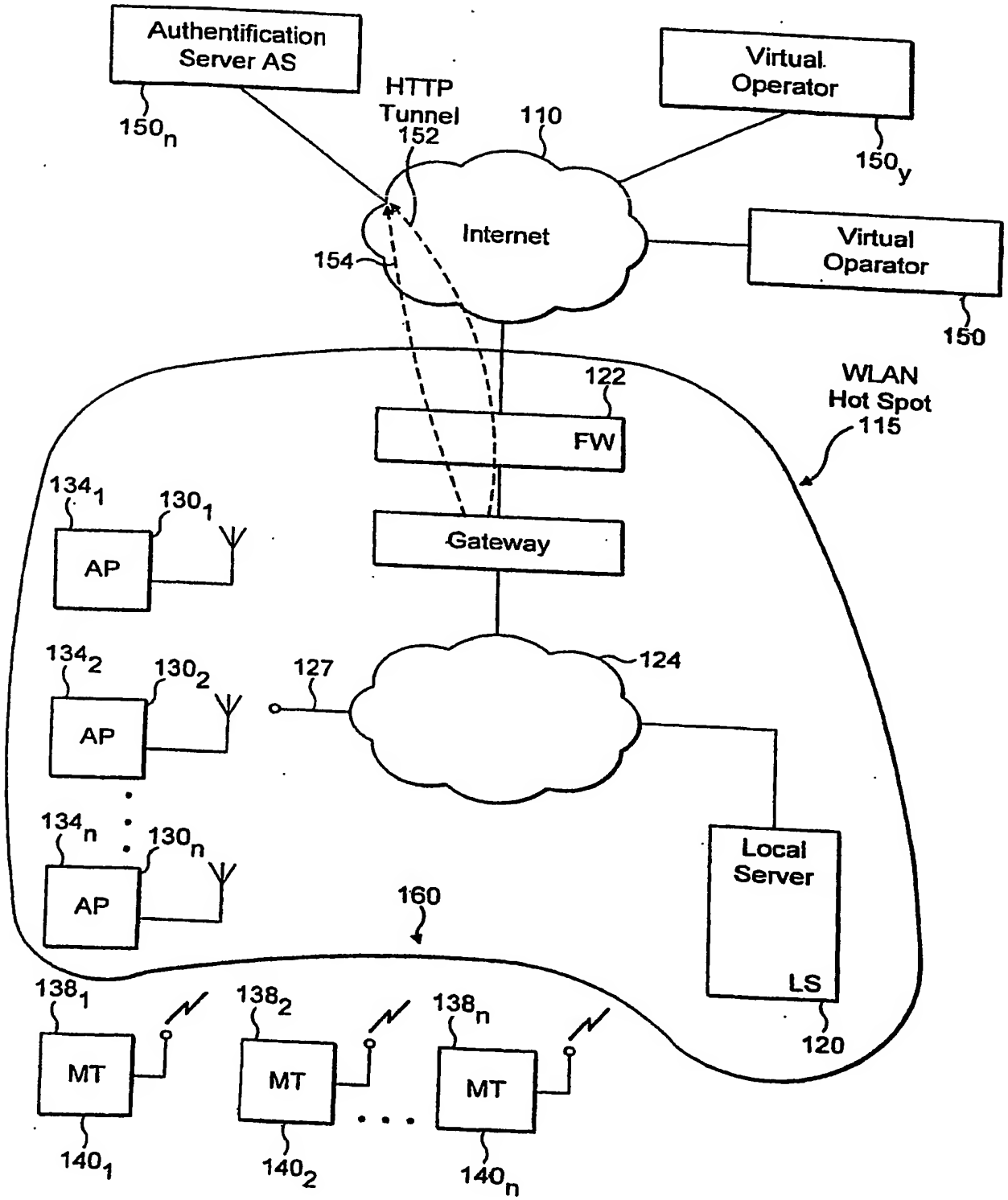
Authentification Server AS
150n
HTTP Tunnel
152
110
Virtual Operator
150y
Internet
154
Virtual Oparator
150
WLAN Hot Spot
115
122
FW
Gateway
1341
1301
AP
1342
1302
AP
127
124
1345
1305
AP
160
Local Server
LS
120
1381
MT
1401
1382
MT
1402
138n
MT
140n

FIG. 1

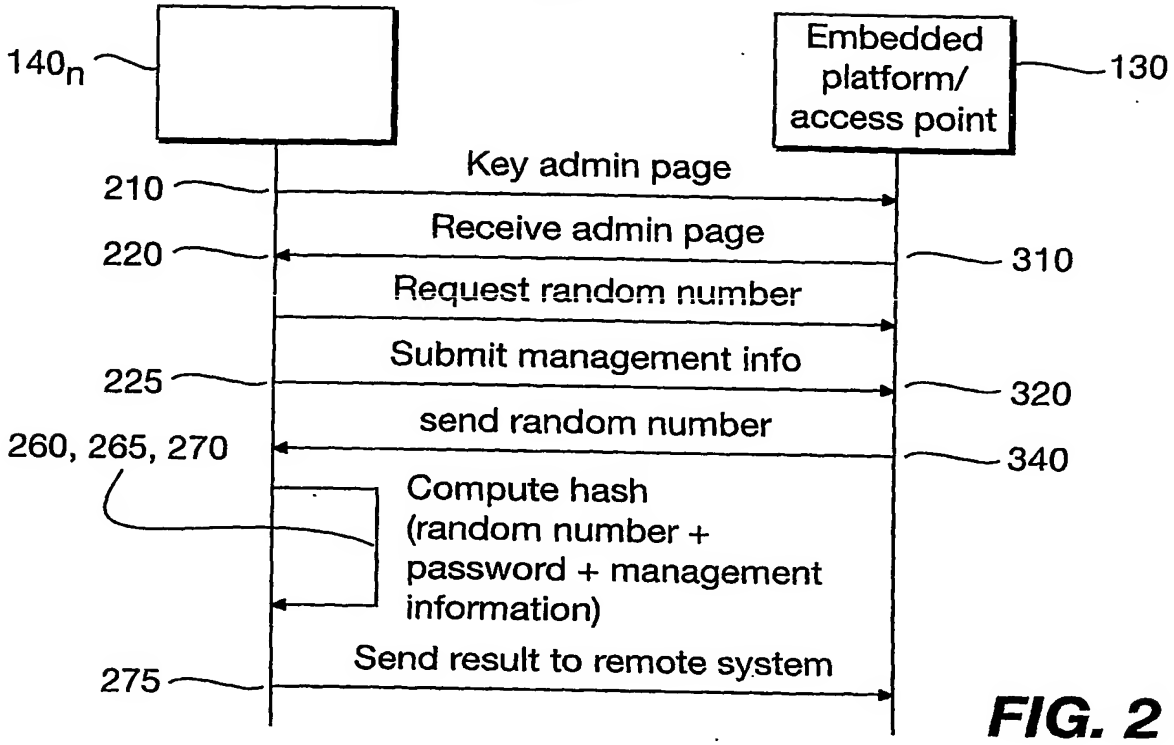
140n
Embedded platform/ access point
130
Key admin page
210
Receive admin page
220
310
Request random number
Submit management info
225
320
send random number
260, 265, 270
340
Compute hash (random number + password + management information)
Send result to remote system
275

FIG. 2

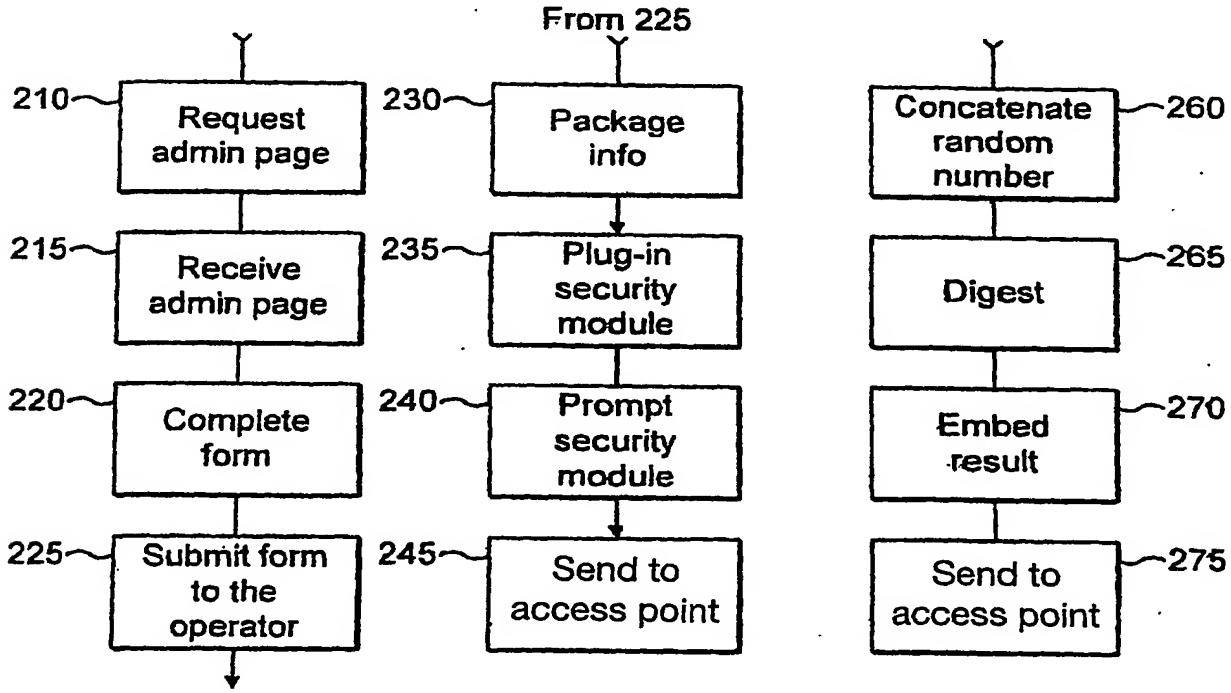
From 225
210
Request admin page
215
Receive admin page
220
Complete form
225
Submit form to the operator
230
Package info
235
Plug-in security module
240
Prompt security module
245
Send to access point
Concatenate random number
260
Digest
265
Embed result
270
Send to access point
275

FIG. 3a

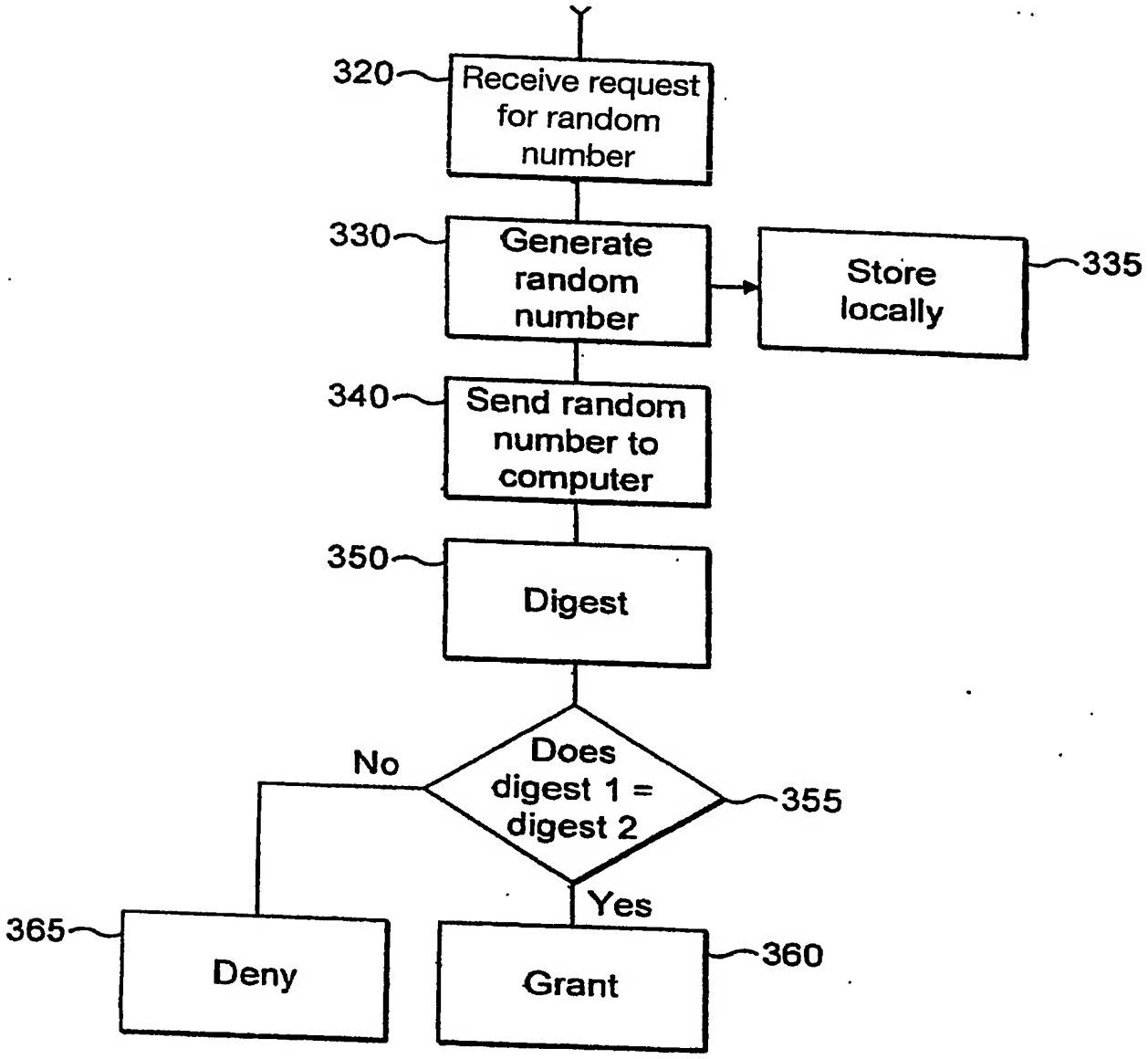
320
Receive request for random number
330
Generate random number
Store locally
335
340
Send random number to computer
350
Digest
No
Does digest 1 = digest 2
355
Yes
365
Deny
Grant
360

FIG. 3b